Bundesamt
für Sicherheit in der
Informationstechnik

OPS.1.1.2 Ordnungsgemäße IT-Administration

1. Beschreibung

1.1. Einleitung

Unter IT-Administration werden Tätigkeiten hauptsächlich innerhalb des IT-Betriebs verstanden, für die administrative Rechte benötigt werden und die die Konfiguration von IT-Komponenten verändern. Administrierende sorgen nicht nur dafür, dass die IT-Komponenten verfügbar bleiben, sondern setzen auch Maßnahmen für die Informationssicherheit um und überprüfen, ob diese wirksam sind.

Zu den Tätigkeitsbereichen der Administrierenden gehört es unter anderem, die IT einer Institution einzurichten, zu konfigurieren, zu überprüfen und bestehende IT zu ändern. Hierzu zählt ebenfalls die Fachadministration, also die IT-Administration von Anwendungen, für deren Betrieb der entsprechende Fachbereich statt der Organisationseinheit IT-Betrieb zuständig ist.

Administrative Rechte für IT-Komponenten (also insbesondere für IT-Systeme, IT-Dienste, Anwendungen, IT-Plattformen und Netze) sind privilegierte Rechte, die neben den Zugängen auch Zugriffe über das Netz sowie physikalische Zutritte umfassen können. Daher sind sowohl die administrativen Rechte auf organisatorischer Ebene als auch die Administrationswerkzeuge selber ein attraktives Ziel für Angreifer. Wesentlich für die Sicherheit der IT-Administration sind die ordnungsgemäße und nachvollziehbare Durchführung aller administrativen Tätigkeiten und die Absicherung der dafür benötigten Hilfsmittel.

1.2. Zielsetzung

Ziel dieses Bausteins ist es, die Informationssicherheit als integralen Bestandteil bei der ordnungsgemäßen IT-Administration zu etablieren. Mit der Umsetzung dieses Bausteins sorgt die Institution einerseits dafür, dass die für die Sicherheit des Informationsverbunds erforderlichen Tätigkeiten der IT-Administration ordnungsgemäß und systematisch durchgeführt werden. Andererseits reagiert die Institution damit auch auf die besonderen Gefährdungen, die sich aus dem Umgang mit privilegierten Rechten und aus dem Zugang zu schützenswerten Bereichen der Institution zwangsläufig ergeben.

1.3. Abgrenzung und Modellierung

Der Baustein OPS.1.1.2 *Ordnungsgemäße IT-Administration* ist einmal auf den gesamten Informationsverbund anzuwenden.

Um ein IT-Grundschutz-Modell für einen konkreten Informationsverbund zu erstellen, muss grundsätzlich die Gesamtheit aller Bausteine betrachtet werden. In der Regel sind mehrere Bausteine auf das Thema bzw. Zielobjekt anzuwenden.

Dieser Baustein behandelt

- übergreifende Anforderungen an den Administrationsprozess, sowohl für den IT-Betrieb als auch in der Fachadministration,
- Anforderungen an administrative Tätigkeiten sowie
- Anforderungen an den Umgang mit administrativen Berechtigungen, also privilegierten Zutritten, Zugängen und Zugriffen.

Folgende Inhalte sind ebenfalls von Bedeutung und werden an anderer Stelle behandelt:

- Fernadministration von IT-Systemen über externe Schnittstellen sowie Fernwartung von Geräten und Komponenten durch die Herstellungs- oder Zulieferunternehmen (siehe OPS.1.2.5 *Fernwartung*)

- Patch- und Änderungsmanagement (siehe OPS.1.1.3 *Patch- und Änderungsmanagement*)
- die Absicherung von Administrationswerkzeugen (siehe NET.1.2 *Netzmanagement* und OPS.1.1.7 *Systemmanagement*)
- die ordnungsgemäße Verwaltung von Benutzenden und Berechtigungen (siehe ORP.4 *Identitäts- und Berechtigungsmanagement*)
- besondere Anforderungen für den Fall, dass die IT-Administration durch Dritte erfolgt (siehe OPS.2.3 *Nutzung von Outsourcing* und OPS.3.2 *Anbieten von Outsourcing*)
- Aspekte für die IT-Administration von industrieller IT (siehe Bausteine aus dem Bereich IND *Industrielle IT*)

Dieser Baustein behandelt **nicht**

- die allgemeinen Aspekte des IT-Betriebs wie Inventarisierung, In- und Außerbetriebnahme von IT-Komponenten sowie die grundsätzlichen Rahmenbedingungen für Administrierende (siehe OPS.1.1.1 *Allgemeiner IT-Betrieb*)
- die Einweisung des Personals in einzuhaltende allgemeine Sicherheitsbestimmungen der IT (siehe ORP.3 *Sensibilisierung und Schulung zur Informationssicherheit*)
- die kontinuierliche Schulung des Personals sowie die damit einhergehende Sensibilisierung für Gefährdungen und Sicherheitsmaßnahmen (siehe ORP.2 *Personal* und ORP.3 *Sensibilisierung und Schulung zur Informationssicherheit*)

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein OPS.1.1.2 *Ordnungsgemäße IT-Administration* von besonderer Bedeutung.

2.1. Unzureichend geregelte Zuständigkeiten

Die IT-Administration umfasst diverse Aufgaben auf verschiedensten Komponenten unterschiedlicher Bereiche. Fehlen Regelungen über Zuständigkeiten oder Prozesse oder sind die Regelungen und Prozesse den Zuständigen nicht bekannt, kann dies verschiedene mögliche Folgen haben. Gegebenenfalls werden erforderliche Administrationsaufgaben gar nicht oder durch den falschen Bereich erledigt, der gegebenenfalls nicht alle zu beachtenden Einzelheiten kennt. Womöglich werden auch gegenwirkende Maßnahmen von verschiedenen Bereichen durchgeführt. Dies kann bewirken, dass IT-Systeme nur eingeschränkt oder gar nicht mehr verfügbar sind.

Wird bei der Festlegung von Zuständigkeiten nicht beachtet, dass verschiedene Administrationstätigkeiten, z. B. zwischen Applikationsbetrieb und Systembetrieb, untrennbar miteinander verbunden sind, können zusammengehörende Aufgaben gegebenenfalls nicht ordnungsgemäß durchgeführt werden.

Erhalten Administrierende zu viele Rechte, weil Zuständigkeiten nicht geregelt sind, können sie eventuell vertrauliche Informationen einsehen, die sie nicht einsehen dürfen. Dies ist insbesondere der Fall, wenn aus Bequemlichkeit zu viele administrative Konten mit zu weitreichenden Rechten eingerichtet sind, im schlimmsten Fall sogar über Organisationseinheiten hinweg.

Außerdem kann eine zu hohe Anzahl Administrierender zu einem Kontrollverlust führen, wenn nicht klar geregelt ist, wer für welche Aufgaben zuständig ist. In diesem Fall sind alle Schutzziele der Informationssicherheit gefährdet.

2.2. Unzureichende Dokumentation

Die Dokumentation kann unzureichend sein, wenn Informationen über IT-Komponenten (z. B. über Konfiguration oder Zugriffsrechte) nicht oder nur unvollständig erfasst wurden. Auch wenn die Dokumentation im Rahmen von Administrationstätigkeiten nicht aktualisiert wird, ist die Dokumentation unzureichend, weil sie nicht mehr dem Ist-Zustand entspricht.

Unzureichende Dokumentation kann zu Fehlkonfigurationen oder allgemein fehlerhafter IT-Administration führen. Dadurch können alle Schutzziele der Informationssicherheit erheblich gefährdet werden.

Außerdem kann auch das Notfallmanagement erheblich beeinträchtigt werden, weil für zeitkritische Aufgaben erst Informationen gesammelt werden müssen oder die Aufgaben aufgrund der Diskrepanz zwischen Dokumentation

und Ist-Zustand nicht wie geplant durchgeführt werden können. Dies kann dazu führen, dass ein Notfall nicht schnell genug behandelt und die Verfügbarkeit von IT-Komponenten länger beeinträchtigt wird.

2.3. Missbrauch von privilegierten Berechtigungen durch Administrierende

Zu weit gefasste administrative Berechtigungen können genutzt werden, um zu sabotieren oder Informationen auszuspähen, die als Ausgangspunkt für Angriffe verwendet werden können. Dadurch werden alle Schutzziele der Informationssicherheit gefährdet.

Privilegierte Zutritte, Zugänge und Zugriffe können auch missbraucht werden, wenn die Prozesse beim Ausscheiden von internen oder externen Administrierenden unzureichend sind und dadurch ausgeschiedene Personen weiterhin auf IT-Komponenten zugreifen können. Auch in diesem Fall sind alle Schutzziele der Informationssicherheit gefährdet.

2.4. Preisgabe von schützenswerten Informationen an unberechtigte Personen

Über Zugänge der IT-Administration kann auf schützenswerte Informationen zugegriffen werden, z. B. auf die Dokumentation, die für die IT-Administration benötigt wird, oder auf die Konfigurationen von IT-Systemen. Werden die Zugänge der IT-Administration unzureichend abgesichert, können auch unberechtigte Personen an schützenswerte Informationen gelangen. Über den Verlust der Vertraulichkeit hinaus können diese Informationen auch manipuliert oder für weitergehende Angriffe genutzt werden, wodurch alle Schutzziele der Informationssicherheit erheblich gefährdet sind.

2.5. Personalausfall von Kernkompetenzträgern

Sind die benötigten Kenntnisse bei den Administrierenden nicht auf allen Gebieten redundant vorhanden, könnte eine entsprechende Administrationstätigkeit nicht durchgeführt werden, wenn Kernkompetenztragende ausfallen. Wenn zusätzlich die Dokumentation für durchzuführende Arbeitsschritte unzureichend ist, kann die Administrationstätigkeit nicht von anderen Administrierenden ohne weitere Risiken durchgeführt werden. Dies kann dazu führen, dass Fehlfunktionen nicht behoben werden können. In der Folge ist die Verfügbarkeit von IT-Systemen nicht (ausreichend) gewährleistet und Schwachstellen können nicht behoben werden, wodurch Angriffe begünstigt werden.

Diese Situation kann auch dadurch entstehen, dass es für Administrationstätigkeiten keine festgelegten Vertretenden mit entsprechenden Berechtigungen gibt oder dass festgelegte Vertretende oder sogar der Notfallzugang nicht über die erforderlichen administrativen Berechtigungen verfügen.

2.6. Unzureichende Verfügbarkeit von Administrierenden

Herrscht bei den Administrierenden Personalmangel, z. B. durch unzureichende Personalplanung, Überbuchung oder Pandemie, können gegebenenfalls erforderliche Administrationsaufgaben nicht durchgeführt werden, falls dazu keine Zeit ist. Unter Umständen werden aufgrund von Zeitmangel auch Fehler bei der IT-Administration gemacht. Beides kann zu unzureichender Verfügbarkeit von IT-Systemen oder zu einer erhöhten Angriffsfläche und damit zur Gefährdung aller Schutzziele der Informationssicherheit führen.

Personalmangel kann zusätzlich zur Folge haben, dass Administrierende aus Zeitmangel für ihre Aufgaben unzureichend geschult werden, was ebenfalls dazu führen kann, dass im Bedarfsfall bzw. im Notfall bestimmte Administrationstätigkeiten nicht korrekt durchgeführt werden.

2.7. Unzureichende Absicherung von Administrationswerkzeugen

Administrationswerkzeuge ermöglichen einen weitreichenden Zugriff auf die IT einer Institution. Werden diese Werkzeuge unzureichend abgesichert, kann das dazu führen, dass die Administrationswerkzeuge als solche bezüglich aller Schutzziele der Informationssicherheit gefährdet sind. Über sie kann die IT-Administration sabotiert werden oder es kann eine unberechtigte IT-Administration ermöglicht werden.

Wird bei einem Angriff Zugriff auf Administrationswerkzeuge erlangt, können weitreichende Berechtigungen erhalten werden. Diese Berechtigungen können für Angriffe aller Art missbraucht werden, wodurch ebenfalls alle Schutzziele der Informationssicherheit gefährdet sind.

Eine Ursache für die unzureichende Absicherung von Administrationswerkzeugen kann z. B. dadurch entstehen, dass sie unzureichend von anderen Anwendungen getrennt sind. Diese unzureichende Trennung ist auf allen Ebe-

nen möglich. Sie kann z. B. dadurch entstehen, dass Texteditoren oder SSH-Clients zur IT-Administration genutzt werden, die auch im nicht-administrativen Kontext verwendet werden.

2.8. Ausfall der Administrationsmöglichkeit

Wenn Administrationsmöglichkeiten ausfallen und es aufgrund von Fehlplanungen keine Redundanz oder andere Alternativen gibt, können Administrationstätigkeiten dieser Art nicht durchgeführt werden, bis der Ausfall behoben ist. Dadurch ist im schlimmsten Fall die gesamte IT eingeschränkt oder nicht verfügbar bzw. funktionstüchtig.

Administrationswerkzeuge können auch durch die Administration des Werkzeuges selbst ausfallen, z. B. durch eine Fehladministration, durch einen eingespielten Patch oder eine Änderung, die durch eine Administrationstätigkeit herbeigeführt wird.

2.9. Fehlgeleitete Administration

Wird die IT-Administration fehlgeleitet, indem z. B. falsche Informationen eingeschleust werden, kann die IT-Administration zu falschen Reaktionen verleitet werden. Beispielsweise können Administrierende außerhalb des geregelten Prozesses fälschlicherweise darüber informiert werden, dass ein IT-System ausgefallen ist, was sie zu einem Neustart verleitet. Hierdurch können Informationen, Hard- oder Software manipuliert werden, wodurch deren Verfügbarkeit und Integrität nicht mehr gewährleistet ist. Zudem können auf diese Weise auch schützenswerte Informationen offengelegt werden.

2.10. Fehlerhafte Administration

Menschliche Fehler können nie ausgeschlossen werden und können bei der IT-Administration weitreichende Folgen haben. Zusätzlich werden sie durch einige der bisher genannten Gefährdungen begünstigt.

Die in der IT-Administration verwendeten Werkzeuge erlauben mit wenig Aufwand sehr weitreichende Änderungen an IT-Komponenten. Je nach Fehler können damit alle Schutzziele der Informationssicherheit erheblich gefährdet sein. Fehler werden insbesondere durch parallele Arbeiten an unterschiedlichen Themen begünstigt, bei denen beispielsweise unterschiedliche Eingabefenster oder Konsolenausgaben verwechselt werden können.

2.11. Störung der IT durch Administrationstätigkeiten

Selbst wenn Administrationstätigkeiten fehlerfrei durchgeführt werden, kann dabei trotzdem die IT der Institution gestört werden. Werden z. B. vorgegebene Wartungsfenster für Administrationstätigkeiten nicht eingehalten, kann die Verfügbarkeit der administrierten IT gestört werden. Zudem können auch korrekt im Wartungsfenster durchgeführte Administrationstätigkeiten später zu Störungen führen, z. B. wenn die Administrierbarkeit der entsprechenden Komponenten durch nicht vorhergesehene Wechselwirkungen beeinträchtigt wird.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins OPS.1.1.2 *Ordnungsgemäße IT-Administration* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeiten	Rollen
Grundsätzlich zuständig	IT-Betrieb
Weitere Zuständigkeiten	Keine

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

OPS.1.1.2.A1 ENTFALLEN (B)

Diese Anforderung ist entfallen.

OPS.1.1.2.A2 Vertretungsregelungen (B)

Für jede Administrationsaufgabe MUSS eine Vertretung benannt werden. Die Vertretung MUSS über die notwendigen administrativen Berechtigungen (organisatorisch und technisch) verfügen, um die Tätigkeit durchführen zu können. Eine benannte Vertretung MUSS über die im Kontext der Administrationsaufgabe notwendigen Kenntnisse verfügen.

Die Regelung der Vertretung MUSS Mangel- und Notfallsituationen berücksichtigen.

OPS.1.1.2.A3 ENTFALLEN (B)

Diese Anforderung ist entfallen.

OPS.1.1.2.A4 Beendigung der Tätigkeit in der IT-Administration (B)

Falls eine Person von Administrationsaufgaben entbunden wird, MÜSSEN ihr alle damit zusammenhängenden privilegierten Berechtigungen auf organisatorischer und technischer Ebene entzogen werden. Insbesondere MÜSSEN persönliche administrative Konten gesperrt und Passwörter aller administrativer Konten geändert werden, die der Person bekannt sind. Weiterhin MÜSSEN alle betroffenen Parteien darauf hingewiesen werden, dass diese Person von den entsprechenden Aufgaben entbunden ist und daher keine administrativen Berechtigungen mehr haben darf.

Es MUSS geregelt werden unter welchen Rahmenbedingungen geprüft wird, ob sich zusätzliche nicht dokumentierte administrative Rechte verschafft wurden. Diese Prüfung SOLLTE insbesondere erfolgen, falls die Entscheidung eine Person von Administrationsaufgaben zu entbinden nicht im Einvernehmen mit der entsprechenden Person getroffen wurde. Falls solche administrativen Rechte gefunden wurden, MÜSSEN diese wieder entzogen werden.

OPS.1.1.2.A5 Nachweisbarkeit von administrativen Tätigkeiten (B)

Administrative Tätigkeiten MÜSSEN nachweisbar sein. Dafür MUSS mindestens festgehalten werden,

- welche Änderung bei einer Tätigkeit durchgeführt wurde,
- wer eine Tätigkeit durchgeführt hat und
- wann eine Tätigkeit durchgeführt wurde.

Die Institution MUSS jederzeit nachweisen können, welche Person welche administrativen Tätigkeiten durchgeführt hat. Dazu SOLLTEN alle Administrierenden über eine eigene Zugangskennung verfügen. Auch Vertretungen von Administrierenden SOLLTEN eigene Zugangskennungen erhalten. Jeder Anmeldevorgang (Login) über eine Administrationskennung MUSS protokolliert werden.

OPS.1.1.2.A6 Schutz administrativer Tätigkeiten (B)

Administrative Schnittstellen und Funktionen DÜRFEN NUR berechtigten Personen zur Verfügung stehen. Für diese Schnittstellen und Funktionen MÜSSEN geeignete Verfahren zur Authentisierung festgelegt werden. Es MUSS sichergestellt sein, dass Administrationstätigkeiten nur durchgeführt werden können, falls vorher eine dementsprechende Authentisierung erfolgt ist.

Es MUSS festgelegt werden, welche Protokolle für Administrationsschnittstellen verwendet werden dürfen, so dass die bei der Administration stattfindende Kommunikation abgesichert ist.

OPS.1.1.2.A21 Regelung der IT-Administrationsrollen (B)

Es MÜSSEN Rollen definiert werden, die ausschließlich zur IT-Administration vergeben werden. Administrationsrollen MÜSSEN aufgrund des tatsächlichen Bedarfs im Aufgabenbereich der IT-Administration nachvollziehbar vergeben werden. Alle notwendigen Administrationstätigkeiten MÜSSEN durch Berechtigungen in den Administrationsrollen nach dem Minimalprinzip abgedeckt sein.

Die IT-Administration unterschiedlicher Ebenen der IT-Komponenten, z. B. die Trennung von Betriebssystem- und Anwendungsadministration, MUSS bei der Konzeption der Administrationsrollen berücksichtigt werden.

OPS.1.1.2.A22 Trennung von administrativen und anderen Tätigkeiten (B)

Die durchführende Person MUSS wissen, bei welchem Teil ihrer Aufgabe es sich um administrative Tätigkeiten handelt. Aufgaben, die keine Administrationsrechte benötigen, DÜRFEN NICHT mit Administrationsrechten ausgeführt werden.

Es MUSS sichergestellt werden, dass Administrationswerkzeuge klar als solche erkennbar sind. Wenn eine Anwendung zur Erfüllung einer Administrationsaufgabe benutzt wird, DARF NICHT dieselbe Instanz dieser Anwendung für andere Aufgaben verwendet werden. Dies SOLLTE auf technischer Ebene sichergestellt werden. Die Zugangskennungen, die zur IT-Administration genutzt werden, SOLLTEN sich von Zugangskennungen unterscheiden, die in anderem Kontext genutzt werden.

3.2. Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für diesen Baustein. Sie SOLLTEN grundsätzlich erfüllt werden.

OPS.1.1.2.A7 Regelung der IT-Administrationstätigkeit (S)

Jede IT-Administrationstätigkeit SOLLTE einer klar definierten Aufgabe zugeordnet sein. Für diese Aufgaben SOLLTE geregelt werden,

- durch wen diese Aufgabe ausgeführt werden darf und
- durch wen diese Aufgabe beauftragt werden darf.

Es SOLLTE nachvollziehbar sein, in welchen Prozessen sich Administrationsaufgaben einfügen. IT-Administrationstätigkeiten SOLLTEN nur mit denjenigen Berechtigungen durchgeführt werden, die zur Erfüllung der entsprechenden Aufgabe notwendig sind. Es SOLLTE festgelegt werden, wie IT-Administrationstätigkeiten auszuführen sind.

Die Regelungen für IT-Administrationstätigkeiten SOLLTEN regelmäßig und anlassbezogen überprüft und aktualisiert werden.

Für jede IT-Administrationstätigkeit SOLLTE sichergestellt werden, dass diese bei Bedarf auch im Notfall ausgeführt werden kann.

OPS.1.1.2.A8 Administration von Fachanwendungen (S)

Es SOLLTE geregelt und dokumentiert werden, welche Administrationsaufgaben für Fachanwendungen vom IT-Betrieb und welche durch die Fachadministration durchgeführt werden.

Für Fachanwendungen SOLLTE identifiziert werden, welche Zugriffe der IT-Betrieb auf Systemebene benötigt.

Alle Schnittstellen und Abhängigkeiten zwischen der Fachadministration und der Administration durch den IT-Betrieb SOLLTEN identifiziert werden. Immer wenn Administrationsprozesse erstellt und gepflegt werden, SOLLTEN die Zuständigkeiten und Abhängigkeiten dieser Schnittstellen berücksichtigt werden.

OPS.1.1.2.A9 ENTFALLEN (S)

Diese Anforderung ist entfallen.

OPS.1.1.2.A10 ENTFALLEN (S)

Diese Anforderung ist entfallen.

OPS.1.1.2.A11 Dokumentation von IT-Administrationstätigkeiten (S)

Durchgeführte Administrationstätigkeiten SOLLTEN nachvollziehbar dokumentiert werden. Es SOLLTE geprüft werden, welche grundsätzlichen Anforderungen an die Dokumentation der Administrationstätigkeiten existieren. Es SOLLTE identifiziert werden, welche Ziele mit der Dokumentation erreicht werden sollen. Aufgrund dieser Anforderungen und Ziele SOLLTE verbindlich festgelegt werden, welche Schritte in welchem Detailierungsgrad dokumentiert werden. Aus der Dokumentation SOLLTE mindestens hervorgehen,

- welche Änderungen erfolgten,
- wann die Änderungen erfolgten,
- wer die Änderungen durchgeführt hat,
- auf welcher Grundlage bzw. aus welchem Anlass die Änderungen erfolgt sind und
- inwiefern und aus welchem Grund gegebenenfalls von vorgegebenen Standards oder Konfigurationen abgewichen wurde.

Dokumentation im Kontext einer Administrationstätigkeit SOLLTE in Standard-Arbeitsabläufen enthalten sein. Es SOLLTE geregelt werden, welche Möglichkeiten zu nutzen sind, falls Administrationstätigkeiten außerplanmäßig durchgeführt werden.

Es SOLLTE identifiziert werden, unter welchen Umständen ein Zugriff auf die Dokumentation notwendig ist. Der Zugriff SOLLTE dementsprechend gewährleistet sein.

OPS.1.1.2.A12 ENTFALLEN (S)

Diese Anforderung ist entfallen.

OPS.1.1.2.A13 ENTFALLEN (S)

Diese Anforderung ist entfallen.

OPS.1.1.2.A16 Erweiterte Sicherheitsmaßnahmen für Administrationszugänge (S)

Der Zugang zu administrativen Oberflächen und Schnittstellen SOLLTE auf IT-Systeme, die zur IT-Administration verwendet werden, beschränkt sein. Daher SOLLTEN Netze, die zur IT-Administration verwendet werden, durch Filter- und Segmentierungsmaßnahmen von produktiven Netzen zu administrierender Komponenten getrennt werden (Out-of-Band-Management). Wo kein Out-of-Band-Management möglich ist, SOLLTEN Software-Schnittstellen und physische Schnittstellen zur IT-Administration durch zusätzliche Maßnahmen abgesichert werden und nur für Personen erreichbar sein, die für deren Nutzung berechtigt sind. Hierzu SOLLTE eine Zwei-Faktor-Authentisierung verwendet werden.

OPS.1.1.2.A20 ENTFALLEN (S)

Diese Anforderung ist entfallen.

OPS.1.1.2.A23 Rollen- und Berechtigungskonzept für administrative Zugriffe (S)

Es SOLLTE ein angemessenes Rollen- und Berechtigungskonzept für administrative Zugriffe existieren. Darin SOLLTEN grundsätzliche Vorgaben gemacht werden, mindestens darüber,

- wie Administrationsrollen beantragt und zugewiesen werden,
- welche Arten von Administrationsrollen existieren,
- welche Arten von Berechtigungen im Kontext der Administrationsrollen vergeben werden,
- wie für die IT-Administration notwendige Berechtigungen vergeben werden.

OPS.1.1.2.A24 Prüfen von Administrationstätigkeiten (S)

Bevor eine Administrationstätigkeit durchgeführt wird, SOLLTE geprüft werden, ob der Anlass und die Art der Tätigkeit im Kontext der zugrundeliegenden Aufgabe plausibel sind. Nachdem eine Administrationstätigkeit an einer Komponente durchgeführt wurde, SOLLTE geprüft werden, ob die Konfiguration und der Status der Komponente dem gewünschten Zielzustand entspricht.

Falls eine zusätzliche Qualitätssicherung der ausgeführten Administrationsaufgabe notwendig ist, SOLLTE diese nicht durch dieselbe Person durchgeführt werden, die die entsprechenden Tätigkeiten durchgeführt hat.

Für Administrationstätigkeiten mit potenziell weitreichenden Folgen SOLLTE geprüft werden, ob diese Tätigkeiten die Verfügbarkeit der IT-Administration selbst einschränken könnten. In diesem Fall SOLLTEN entsprechende Vorkehrungen getroffen werden, um einen Rollback der Administrationstätigkeiten zu ermöglichen.

OPS.1.1.2.A25 Zeitfenster für schwerwiegende Administrationstätigkeiten (S)

Für Administrationstätigkeiten mit potenziell weitreichenden Folgen SOLLTEN durch den IT-Betrieb Wartungsfenster abgestimmt werden. Falls der IT-Betrieb für Administrationstätigkeiten Vorgaben zu Zeitfenstern macht, MÜSSEN diese eingehalten werden.

OPS.1.1.2.A26 Backup der Konfiguration (S)

Alle Konfigurationen SOLLTEN durch regelmäßige Backups auf Anwendungsebene und auf IT-Systemebene gesichert werden. Vor Administrationstätigkeiten mit potenziell weitreichenden Folgen SOLLTE ein zusätzliches Backup gemacht werden. Für Backups SOLLTE gewährleistet sein, dass sie im Fehlerfall wieder eingespielt werden können.

OPS.1.1.2.A27 Ersatz für zentrale IT-Administrationswerkzeuge (S)

Für zentrale IT-Administrationswerkzeuge SOLLTEN Alternativen zur Verfügung stehen, mit denen im Bedarfsfall administriert werden kann. Hierzu SOLLTEN Sprungsysteme mit Zugriff auf entsprechende Administrationsnetze zur Verfügung stehen. Falls solche Alternativen nicht zur Verfügung stehen, SOLLTE zur IT-Administration der Zugang und der direkte Zugriff auf die zu administrierende IT möglich sein.

OPS.1.1.2.A28 Protokollierung administrativer Tätigkeiten (S)

Administrative Tätigkeiten SOLLTEN protokolliert werden. Die Protokolldateien SOLLTEN für eine angemessene Zeitdauer geschützt aufbewahrt werden. Die ausführenden Administrierenden SOLLTEN keine Möglichkeiten haben, die aufgezeichneten Protokolldateien zu verändern oder zu löschen. Protokolldaten SOLLTEN regelmäßig geprüft werden.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

OPS.1.1.2.A14 ENTFALLEN (H)

Diese Anforderung ist entfallen.

OPS.1.1.2.A15 ENTFALLEN (H)

Diese Anforderung ist entfallen.

OPS.1.1.2.A17 IT-Administration im Vier-Augen-Prinzip (H)

Es SOLLTE geregelt werden, welche Administrationsaufgaben eine zusätzliche Person erfordern, die die Ausführung überwacht. Diese Person SOLLTE im Kontext der durchzuführenden Administrationstätigkeiten auch über die zur Ausführung notwendigen Qualifikationen verfügen.

OPS.1.1.2.A18 Durchgängige Protokollierung administrativer Tätigkeiten (H)

Bei IT-Komponenten mit hohem Schutzbedarf SOLLTEN alle administrativen Tätigkeiten in sämtlichen Bereichen protokolliert werden. Dabei SOLLTE jede administrative Aktion vollständig nachvollzogen werden. Die ausführenden Administrierenden SOLLTEN keinen Einfluss auf Art und Umfang der Protokollierung nehmen können.

OPS.1.1.2.A19 Nutzung hochverfügbarer IT-Administrationswerkzeuge (H)

Administrationswerkzeuge SOLLTEN redundant ausgelegt werden. Es SOLLTE sichergestellt werden, dass im Störungsfall weiterhin alle Administrationsaufgaben ohne wesentliche Einschränkungen ausgeführt werden können.

OPS.1.1.2.A29 Monitoring der IT-Administrationswerkzeuge (H)

Für IT-Administrationswerkzeuge SOLLTEN Kenngrößen zur Verfügbarkeit identifiziert werden. Diese Kenngrößen SOLLTEN kontinuierlich überwacht werden. Es SOLLTEN tolerierbare Grenzwerte dieser Kenngrößen festgelegt werden. Werden diese nicht eingehalten, SOLLTEN die zuständigen Teams automatisch benachrichtigt werden.

OPS.1.1.2.A30 Sicherheitsmonitoring administrativer Tätigkeiten (H)

Falls ein IT-System zur zentralen Detektion und automatisierten Echtzeitüberprüfung von Ereignismeldungen genutzt wird, SOLLTEN dort Ereignisdaten zu administrativen Tätigkeiten ausgewertet werden. Hierzu SOLLTEN bestehende Monitoring-Systeme der IT sowie kritische Administrationswerkzeuge in dieses IT-System eingebunden werden.

4. Weiterführende Informationen

4.1. Wissenswertes

Die International Organization for Standardization (ISO) stellt in Anhang A der Norm ISO/IEC 27001:2013 unter anderem im Kontext der Themen Zugangssteuerung (A.9) und IT-Betrieb (A.12) Anforderungen an die ordnungsgemäße IT-Administration.

Das BSI spezifiziert unter anderem für den Bereich der sicheren Administration Anforderungen im Dokument „Konkretisierung der Anforderungen an die gemäß § 8a Absatz 1 BSIG umzusetzenden Maßnahmen".

Bundesamt
für Sicherheit in der
Informationstechnik

OPS.1.1.3 Patch- und Änderungsmanagement

1. Beschreibung

1.1. Einleitung

Es ist eine große Herausforderung, die in einer Institution eingesetzten Komponenten der Informationstechnik korrekt und zeitnah zu aktualisieren. So zeigt sich in der Praxis, dass vorhandene Sicherheitslücken oder Betriebsstörungen häufig auf mangelhafte oder fehlende Patches und Änderungen zurückzuführen sind. Ein fehlendes oder vernachlässigtes Patch- und Änderungsmanagement führt daher schnell zu möglichen Angriffspunkten.

Aufgabe des Patch- und Änderungsmanagements ist es allgemein, verändernde Eingriffe in Anwendungen, Infrastruktur, Dokumentationen, Prozesse und Verfahren steuer- und kontrollierbar zu gestalten.

1.2. Zielsetzung

In diesem Baustein wird aufgezeigt, wie ein funktionierendes Patchmanagement in einer Institution aufgebaut und wie der entsprechende Prozess kontrolliert und optimiert werden kann.

Über das Patchmanagement hinaus beinhaltet der Baustein jedoch auch einige Kernaspekte eines Änderungsmanagements, die für die Informationssicherheit relevant sind. Mit Änderungsmanagement wird die Aufgabe bezeichnet, Änderungen zu planen und zu steuern.

1.3. Abgrenzung und Modellierung

Der Baustein OPS.1.1.3 *Patch- und Änderungsmanagement* ist für den gesamten Informationsverbund anzuwenden.

Die Beschreibungen in diesem Baustein konzentrieren sich auf den IT-Betrieb, und dort insbesondere auf das Patchmanagement, mit dem Software aktualisiert wird (z. B. durch Sicherheitskorrekturen, Service Packs und Hot Fixes). In den einzelnen Bausteinen der Schichten SYS *IT-Systeme* und APP *Anwendungen* finden sich gegebenenfalls spezifischere Anforderungen bezüglich des Patch- und Änderungsmanagements.

Dieser Baustein beinhaltet kein vollständiges Änderungsmanagement, sondern lediglich die Kernaspekte zur Informationssicherheit. In größeren Institutionen ist es sinnvoll, darüber hinaus ein Änderungsmanagement systematisch zu strukturieren. Hierzu können Standardwerke, wie z. B. der Change-Management-Prozess der „IT Infrastructure Library“ (ITIL), herangezogen werden. Ein solches Änderungsmanagement muss nicht auf die IT beschränkt sein, sondern kann auch Geschäftsprozesse und Fachaufgaben selbst umfassen. Unter Änderung wird in diesem Baustein alles inbegriffen, was damit einhergeht, IT-Komponenten anzupassen, wie z. B. „Changes“, „Patches“, „Updates“, „Upgrades“, „Einbau“, „Ausbau“, etc. Software Entwicklung hingegen wird im Baustein CON.8 *Software-Entwicklung* betrachtet.

Anforderungen zu Test und Freigabe von Patches und Software werden in diesem Baustein nicht im Detail behandelt. Sie finden sich im Baustein OPS.1.1.6 *Software-Tests und -Freigaben.*

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein OPS.1.1.3 *Patch- und Änderungsmanagement* von besonderer Bedeutung.

2.1. Mangelhaft festgelegte Zuständigkeiten

Durch mangelhaft festgelegte, sich überschneidende oder ungeklärte Zuständigkeiten können beispielsweise Änderungsanforderungen langsamer kategorisiert und priorisiert werden. Dadurch kann sich insgesamt die Verteilung von Patches und Änderungen verzögern. Auch wenn Patches und Änderungen vorschnell ohne Testlauf und Berücksichtigung aller (fachlichen) Aspekte freigegeben werden, kann sich das gravierend auf die Sicherheit auswirken.

Im Extremfall können mangelhaft festgelegte Zuständigkeiten die gesamte Institution komplett oder in großem Umfang beeinträchtigen. Störungen im Betrieb wirken sich negativ auf die Verfügbarkeit aus. Werden sicherheitsrelevante Patches nicht oder verspätet verteilt, können die Vertraulichkeit und Integrität gefährdet werden.

2.2. Mangelhafte Kommunikation beim Änderungsmanagement

Wenn das Patch- und Änderungsmanagement innerhalb der Institution wenig akzeptiert wird oder die beteiligten Personen mangelhaft kommunizieren, kann das dazu führen, dass Änderungsanforderungen verzögert bearbeitet werden oder über eine Änderungsanforderung falsch entschieden wird. Dadurch kann das Sicherheitsniveau insgesamt verringert und der IT-Betrieb ernsthaft gestört werden. In jedem Fall wird bei mangelhafter Kommunikation der Änderungsprozess ineffizient, da zu viel Zeit und Ressourcen investiert werden müssen. Dies wirkt sich negativ auf die Reaktionsfähigkeit der Institution aus und kann im Extremfall dazu führen, dass Sicherheitslücken entstehen oder wichtige Ziele der Institution nicht erreicht werden.

2.3. Mangelhafte Berücksichtigung von Geschäftsprozessen und Fachaufgaben

Ungeeignete Änderungen können unter anderem den reibungslosen Ablauf der Geschäftsprozesse oder Fachaufgaben beeinträchtigen oder gar dazu führen, dass die beteiligten IT-Systeme komplett ausfallen. Auch ein noch so umfangreiches Testverfahren kann nicht vollkommen ausschließen, dass sich eine Änderung im späteren Produktivbetrieb als fehlerhaft erweist.

Wird im Änderungsprozess die Auswirkung, Kategorie oder Priorität einer eingereichten Änderungsanforderung hinsichtlich der Geschäftsprozesse beziehungsweise Fachaufgaben falsch eingeschätzt, kann sich das angestrebte Sicherheitsniveau verringern. Solche Fehleinschätzungen treten überwiegend auf, wenn sich die für die IT zuständigen Personen und die zuständigen Fachabteilungen nicht ausreichend abstimmen.

2.4. Unzureichende Ressourcen beim Patch- und Änderungsmanagement

Für ein wirkungsvolles Patch- und Änderungsmanagement sind angemessene personelle, zeitliche und finanzielle Ressourcen erforderlich. Sind diese nicht vorhanden, könnten beispielsweise die notwendigen Rollen mit ungeeigneten Personen besetzt werden. Auch können so keine Schnittstellen für bestimmte Informationen geschaffen werden, beispielsweise zwischen der IT und den entsprechenden Ansprechpartnern und Ansprechpartnerinnen in den Fachbereichen. Auch die erforderlichen Kapazitäten für die Infrastruktur der Test- und Verteilungsumgebungen könnten nicht bereitgestellt werden. Können die personellen, zeitlichen und finanziellen Mängel im Regelbetrieb häufig noch ausgeglichen werden, zeigen sie sich unter hohem Zeitdruck umso deutlicher, beispielsweise wenn Notfallpatches eingespielt werden müssen.

2.5. Probleme bei der automatisierten Verteilung von Patches und Änderungen

Häufig werden Patches und Änderungen nicht manuell, sondern zentral softwareunterstützt verteilt. Wird eine solche Software benutzt, können fehlerhafte Patches und Änderungen automatisiert im gesamten Informationsverbund verteilt werden, wodurch große Sicherheitsprobleme entstehen können. Besonders gravierend ist es, wenn auf vielen IT-Systemen gleichzeitig Software installiert wird, die Sicherheitslücken enthält.

Treten nur vereinzelte Fehler auf, lassen sie sich oft per Hand beheben. Problematisch wird es aber, wenn IT-Systeme über einen längeren Zeitraum nicht erreichbar sind. Ein Beispiel sind Mitarbeitende im Außendienst, die ihre IT-Systeme nur selten und unregelmäßig an das LAN der Institution anschließen. Wenn das Werkzeug so konfiguriert wird, dass die Aktualisierungen nur innerhalb eines bestimmten Zeitraums verteilt werden, und dann nicht alle IT-Systeme erreichbar sind, können diese IT-Systeme nicht aktualisiert werden.

2.6. Mangelhafte Wiederherstellungsoptionen beim Patch- und Änderungsmanagement

Wenn Patches oder Änderungen verteilt werden, ohne dass eine Wiederherstellungsoption vorgesehen ist, oder wenn die Wiederherstellungsroutinen der eingesetzten Software nicht oder nicht angemessen wirken, kann fehlerhaft aktualisierte Software nicht zeitnah korrigiert werden. Dadurch können wichtige IT-Systeme ausfallen und hohe Folgeschäden entstehen. Neben dem Verlust der Daten sind vor allem die Verfügbarkeit und Integrität der Daten und der betroffenen IT-Systeme gefährdet.

2.7. Fehleinschätzung der Relevanz von Patches und Änderungen

Werden Änderungen falsch priorisiert, könnten beispielsweise zuerst unwichtige Patches installiert werden. Wichtige Patches hingegen werden dann zu spät installiert. Sicherheitslücken bleiben so länger bestehen. Das Patch- und Änderungsmanagement wird oft durch softwarebasierte Werkzeuge unterstützt. Auch diese Werkzeuge können Softwarefehler enthalten und dadurch unzureichende oder fehlerhafte Angaben über eine Änderung machen. Werden die Angaben, die ein solches Tool über eine Änderung macht, nicht überprüft und auf Plausibilität getestet, kann die tatsächliche von der angenommenen Umsetzung von Änderungen abweichen.

2.8. Manipulation von Daten und Werkzeugen beim Änderungsmanagement

Das Patch- und Änderungsmanagement agiert oft von zentraler Stelle aus. Aufgrund seiner exponierten Stellung ist es besonders gefährdet. Wenn es bei einem Angriff gelingen sollte, die beteiligten Server zu übernehmen, könnten über diesen zentralen Punkt manipulierte Softwareversionen gleichzeitig auf eine Vielzahl von IT-Systemen verteilt werden. Oft entstehen weitere Angriffspunkte dadurch, dass diese IT-Systeme von externen Partnerinstitutionen betrieben werden (Outsourcing). Es könnte auch Wartungszugänge geben, die ermöglichen, auf den zentralen Server zur Verteilung von Änderungen zuzugreifen. Auch diese könnten für Angriffe genutzt werden.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins OPS.1.1.3 *Patch- und Änderungsmanagement* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeiten	Rollen
Grundsätzlich zuständig	IT-Betrieb
Weitere Zuständigkeiten	Fachverantwortliche

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

OPS.1.1.3.A1 Konzept für das Patch- und Änderungsmanagement (B) [Fachverantwortliche]

Wenn IT-Komponenten, Software oder Konfigurationsdaten geändert werden, MUSS es dafür Vorgaben geben, die auch Sicherheitsaspekte berücksichtigen. Diese MÜSSEN in einem Konzept für das Patch- und Änderungsmanagement festgehalten und befolgt werden. Alle Patches und Änderungen MÜSSEN geeignet geplant, genehmigt und dokumentiert werden. Patches und Änderungen SOLLTEN vorab geeignet getestet werden (siehe hierzu auch OPS.1.1.6 *Software-Tests und Freigaben*). Wenn Patches installiert und Änderungen durchgeführt werden, MÜSSEN Rückfall-Lösungen vorhanden sein. Bei größeren Änderungen MUSS zudem der oder die ISB beteiligt sein. Insgesamt MUSS sichergestellt werden, dass das angestrebte Sicherheitsniveau während und nach den Änderungen erhalten bleibt. Insbesondere SOLLTEN auch die gewünschten Sicherheitseinstellungen erhalten bleiben.

OPS.1.1.3.A2 Festlegung der Zuständigkeiten (B)

Für alle Organisationsbereiche MÜSSEN Zuständige für das Patch- und Änderungsmanagement festgelegt werden. Die definierten Zuständigkeiten MÜSSEN sich auch im Berechtigungskonzept widerspiegeln.

OPS.1.1.3.A3 Konfiguration von Autoupdate-Mechanismen (B)

Innerhalb der Strategie zum Patch- und Änderungsmanagement MUSS definiert werden, wie mit integrierten Update-Mechanismen (Autoupdate) der eingesetzten Software umzugehen ist. Insbesondere MUSS festgelegt werden, wie diese Mechanismen abgesichert und passend konfiguriert werden. Außerdem SOLLTEN neue Komponenten daraufhin überprüft werden, welche Update-Mechanismen sie haben.

OPS.1.1.3.A15 Regelmäßige Aktualisierung von IT-Systemen und Software (B)

IT-Systeme und Software SOLLTEN regelmäßig aktualisiert werden.

Grundsätzlich SOLLTEN Patches zeitnah nach Veröffentlichung eingespielt werden. Basierend auf dem Konzept für das Patch- und Änderungsmanagement MÜSSEN Patches zeitnah nach Veröffentlichung bewertet und entsprechend priorisiert werden. Für die Bewertung SOLLTE geprüft werden, ob es zu diesem Patch bekannte Schwachstellen gibt. Es MUSS entschieden werden, ob der Patch eingespielt werden soll. Wenn ein Patch eingespielt wird, SOLLTE kontrolliert werden, ob dieser auf allen relevanten Systemen zeitnah erfolgreich eingespielt wurde. Wenn ein Patch nicht eingespielt wird, MÜSSEN die Entscheidung und die Gründe dafür dokumentiert werden.

Falls Hardware- oder Software-Produkte eingesetzt werden sollen, die nicht mehr von den Herstellenden unterstützt werden oder für die kein Support mehr vorhanden ist, MUSS geprüft werden, ob diese dennoch sicher betrieben werden können. Ist dies nicht der Fall, DÜRFEN diese Hardware- oder Software-Produkte NICHT mehr verwendet werden.

OPS.1.1.3.A16 ENTFALLEN (B)

Diese Anforderung ist entfallen.

3.2. Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für diesen Baustein. Sie SOLLTEN grundsätzlich erfüllt werden.

OPS.1.1.3.A4 ENTFALLEN (S)

Diese Anforderung ist entfallen.

OPS.1.1.3.A5 Umgang mit Änderungsanforderungen (S) [Fachverantwortliche]

Alle Änderungsanforderungen (Request for Changes, RfCs) SOLLTEN erfasst und dokumentiert werden. Die Änderungsanforderungen SOLLTEN von den jeweiligen Fachverantwortlichen für das Patch- und Änderungsmanagement daraufhin kontrolliert werden, ob die Aspekte der Informationssicherheit ausreichend berücksichtigt wurden.

OPS.1.1.3.A6 Abstimmung von Änderungsanforderungen (S)

Der zu einer Änderung zugehörige Abstimmungsprozess SOLLTE alle relevanten Zielgruppen und die Auswirkungen auf die Informationssicherheit berücksichtigen. Die von der Änderung betroffenen Zielgruppen SOLLTEN sich nachweisbar dazu äußern können. Auch SOLLTE es ein festgelegtes Verfahren geben, wodurch wichtige Änderungsanforderungen beschleunigt werden können.

OPS.1.1.3.A7 Integration des Änderungsmanagements in die Geschäftsprozesse (S)

Der Änderungsmanagementprozess SOLLTE in die Geschäftsprozesse beziehungsweise Fachaufgaben integriert werden. Bei geplanten Änderungen SOLLTE die aktuelle Situation der davon betroffenen Geschäftsprozesse berücksichtigt werden. Alle relevanten Fachabteilungen SOLLTEN über anstehende Änderungen informiert werden. Auch SOLLTE es eine Eskalationsebene geben, deren Mitglieder der Leitungsebene der Institution angehören. Die Mitglieder dieser Eskalationsebene SOLLTEN in Zweifelsfällen über Priorität und Terminplanung einer Hard- oder Software-Änderung entscheiden.

OPS.1.1.3.A8 Sicherer Einsatz von Werkzeugen für das Patch- und Änderungsmanagement (S)

Anforderungen und Rahmenbedingungen SOLLTEN definiert werden, nach denen Werkzeuge für das Patch- und Änderungsmanagement ausgewählt werden. Außerdem SOLLTE eine spezifische Sicherheitsrichtlinie für die eingesetzten Werkzeuge erstellt werden.

OPS.1.1.3.A9 Test- und Abnahmeverfahren für neue Hardware (S)

Wenn neue Hardware ausgewählt wird, SOLLTE geprüft werden, ob die eingesetzte Software und insbesondere die relevanten Betriebssysteme mit der Hardware und deren Treibersoftware kompatibel sind. Neue Hardware SOLLTE getestet werden, bevor sie eingesetzt wird. Diese SOLLTE ausschließlich in einer isolierten Umgebung getestet werden.

Für IT-Systeme SOLLTE es ein Abnahmeverfahren und eine Freigabeerklärung geben. Die Zuständigen SOLLTEN die Freigabeerklärungen an geeigneter Stelle schriftlich hinterlegen. Für den Fall, dass trotz der Abnahme- und Freigabeverfahren im laufenden Betrieb Fehler festgestellt werden, SOLLTE es ein Verfahren zur Fehlerbehebung geben.

OPS.1.1.3.A10 Sicherstellung der Integrität und Authentizität von Softwarepaketen (S)

Während des gesamten Patch- oder Änderungsprozesses SOLLTE die Authentizität und Integrität von Softwarepaketen sichergestellt werden. Dazu SOLLTE geprüft werden, ob für die eingesetzten Softwarepakete Prüfsummen oder digitale Signaturen verfügbar sind. Falls ja, SOLLTEN diese vor der Installation des Pakets überprüft werden. Ebenso SOLLTE darauf geachtet werden, dass die notwendigen Programme zur Überprüfung vorhanden sind.

Software und Updates SOLLTEN grundsätzlich nur aus vertrauenswürdigen Quellen bezogen werden.

OPS.1.1.3.A11 Kontinuierliche Dokumentation der Informationsverarbeitung (S)

Änderungen SOLLTEN in allen Phasen, allen Anwendungen und allen Systemen dokumentiert werden. Dazu SOLLTEN entsprechende Regelungen erarbeitet werden.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

OPS.1.1.3.A12 Einsatz von Werkzeugen beim Änderungsmanagement (H)

Bevor ein Werkzeug zum Änderungsmanagement benutzt wird, SOLLTE sorgfältig geprüft werden, ob damit die Änderungen angemessen im Informationsverbund verteilt werden können. Zusätzlich SOLLTEN Unterbrechungspunkte definiert werden können, an denen die Verteilung einer fehlerhaften Änderung gestoppt wird.

OPS.1.1.3.A13 Erfolgsmessung von Änderungsanforderungen (H) [Fachverantwortliche]

Um zu überprüfen, ob eine Änderung erfolgreich war, SOLLTEN die jeweiligen Fachverantwortlichen für das Patch- und Änderungsmanagement sogenannte Nachtests durchführen. Dazu SOLLTEN sie geeignete Referenzsysteme als Qualitätssicherungssysteme auswählen. Die Ergebnisse der Nachtests SOLLTEN im Rahmen des Änderungsprozesses dokumentiert werden.

OPS.1.1.3.A14 Synchronisierung innerhalb des Änderungsmanagements (H)

Im Änderungsmanagementprozess SOLLTE durch geeignete Mechanismen sichergestellt werden, dass auch zeitweise oder längerfristig nicht erreichbare Geräte die Patches und Änderungen erhalten.

4. Weiterführende Informationen

4.1. Wissenswertes

Die International Organization for Standardization (ISO) gibt in der Norm ISO/IEC 27001:2013 im Kapitel 12.1.2 Change Management Vorgaben, die für das Patch- und Änderungsmanagement relevant sind.

Die IT Infrastructure Library (ITIL) gibt Hinweise zum Aufbau eines Change-Management-Prozesses.

Bundesamt
für Sicherheit in der
Informationstechnik

OPS.1.1.4 Schutz vor Schadprogrammen

1. Beschreibung

1.1. Einleitung

Schadprogramme sind Programme, die in der Regel ohne Wissen und Einwilligung der Benutzenden schädliche Funktionen auf einem IT-System ausführen. Diese Schadfunktionen können ein breites Feld abdecken, das von Spionage über Erpressung (sogenannte Ransomware) bis hin zur Sabotage und Zerstörung von Informationen oder gar Geräten reicht.

Schadprogramme können grundsätzlich auf allen Betriebssystemen und IT-Systemen ausgeführt werden. Dazu gehören neben klassischen IT-Systemen wie Clients und Servern auch mobile Geräte wie Smartphones. Netzkomponenten wie Router, Industriesteuerungsanlagen und sogar IoT-Geräte wie vernetzte Kameras sind heutzutage ebenfalls vielfach durch Schadprogramme gefährdet.

Schadprogramme verbreiten sich auf klassischen IT-Systemen zumeist über E-Mail-Anhänge, manipulierte Webseiten (Drive-by-Downloads) oder Datenträger. Smartphones werden in der Regel über die Installation von schädlichen Apps infiziert, auch Drive-by-Downloads sind möglich. Darüber hinaus sind offene Netzschnittstellen, fehlerhafte Konfigurationen und Softwareschwachstellen häufige Einfallstore auf allen IT-Systemen.

In diesem Baustein wird der Begriff „Virenschutzprogramm" verwendet. „Viren" stehen dabei als Synonym für alle Arten von Schadprogrammen. Gemeint ist mit „Virenschutzprogramm" demnach ein Programm zum Schutz vor jeglicher Art von Schadprogrammen.

1.2. Zielsetzung

Dieser Baustein beschreibt Anforderungen, die zu erfüllen und umzusetzen sind, um eine Institution effektiv gegen Schadprogramme zu schützen.

1.3. Abgrenzung und Modellierung

Der Baustein OPS.1.1.4 *Schutz vor Schadprogrammen* ist einmal auf den Informationsverbund anzuwenden.

In diesem Baustein werden die allgemeinen Anforderungen für den Schutz gegen Schadprogramme beschrieben. Spezifische Anforderungen, um bestimmte IT-Systeme der Institution vor Schadprogrammen zu schützen, finden sich bei Bedarf in den jeweiligen Bausteinen der Schicht SYS *IT-Systeme.* Führt ein identifiziertes Schadprogramm zu einem Sicherheitsvorfall, sollten die Anforderungen des Bausteins DER.2.1 *Behandlung von Sicherheitsvorfällen* berücksichtigt werden. Die Anforderungen des Bausteins DER.2.3 *Bereinigung weitreichender Sicherheitsvorfälle* helfen dabei, identifizierte Schadprogramme zu entfernen und einen bereinigten Zustand wiederherzustellen.

Die im Rahmen dieses Bausteins eingesetzten Virenschutzprogramme sollten grundsätzlich auch im Patch- und Änderungsmanagement (OPS.1.1.3 *Patch- und Änderungsmanagement*) berücksichtigt werden. Weiterhin sollte das Thema Schutz vor Schadprogrammen im Rahmen des Bausteins ORP.3 *Sensibilisierung und Schulung zur Informationssicherheit* und CON.3 *Datensicherungskonzept* mit berücksichtigt werden.

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein OPS.1.1.4 *Schutz vor Schadprogrammen* von besonderer Bedeutung.

2.1. Softwareschwachstellen und Drive-by-Downloads

Sind IT-Systeme nicht ausreichend vor Schadprogrammen geschützt, können Softwareschwachstellen bei Angriffen ausgenutzt werden, um Schadcode auszuführen. Dies kann unter anderem passieren, wenn Patches nicht zeitnah eingespielt und Schutzmechanismen von Anwendungsprogrammen, wie Browsern, nicht richtig konfiguriert sind. Bei den sogenannten Drive-by-Downloads reicht es beispielsweise aus, eine mit Schadcode behaftete Website zu besuchen. Eine Schwachstelle im Browser oder in einem installierten Plug-in, wie Java oder Adobe Flash, kann dann ausgenutzt werden, um das IT-System zu infizieren und Angreifenden umfangreiche Kontrolle sowie einen Zugang zum Netz einer Institution zu verschaffen. Besonders gefährdet sind hier IT-Systeme, die nicht regelmäßig aktualisiert werden, z. B. viele Smartphones.

2.2. Erpressung durch Ransomware

Eine weitverbreitete Art von Schadprogrammen ist die sogenannte Ransomware. Diese verschlüsselt die Daten des infizierten IT-Systems sowie häufig auch weitere Daten, die etwa über Netzfreigaben erreichbar sind. In der Regel verwenden die Angreifenden dabei Verschlüsselungsmethoden, die ohne Kenntnis des Schlüssels nicht umkehrbar sind, und erpressen damit ihre Opfer um hohe Geldsummen. Besteht kein wirksamer Schutz gegen Schadprogramme und sind keine ergänzenden Vorkehrungen, wie Datensicherungen, getroffen, kann die Verfügbarkeit von Informationen erheblich eingeschränkt werden, Daten können verloren gehen, sowie massive finanzielle und Image-Schäden können eintreten.

2.3. Gezielte Angriffe und Social Engineering

Institutionen werden häufig mit maßgeschneiderten Schadprogrammen angegriffen. Dabei werden z. B. Führungskräfte über Methoden des Social Engineerings dazu verleitet, schädliche E-Mail-Anhänge zu öffnen. Maßgeschneiderte Schadprogramme können zudem häufig nicht unmittelbar von Virenschutzprogrammen erkannt werden. Auch die Personalabteilung einer Institution kann beispielsweise ein Angriffsziel sein, indem etwa mit Schadsoftware infizierte Bewerbungsunterlagen auf elektronischem Wege zugesendet werden. Konnten die Angreifenden auf diese Weise ein IT-System infizieren, so können sie sich innerhalb der Institution ausbreiten und beispielsweise Informationen einsehen, manipulieren oder zerstören.

2.4. Botnetze

Über Schadprogramme können IT-Systeme einer Institution Teil von sogenannten Botnetzen werden. Angreifende, die in einem solchen Botnetz häufig tausende von Systemen kontrollieren, können diese beispielsweise einsetzen, um Spam zu versenden oder verteilte Denial-of-Service (DDoS)-Angriffe auf Dritte zu starten. Auch wenn die eigene Institution möglicherweise nicht unmittelbar geschädigt wird, kann sich dies trotzdem negativ bezüglich der Verfügbarkeit und Integrität der eigenen Dienste und IT-Systeme auswirken und sogar rechtliche Probleme nach sich ziehen. Wenn z. B. der E-Mail-Server einer Institution auf eine Blockliste gelangt, ist möglicherweise kein Versand und Empfang von E-Mails mehr möglich.

2.5. Infektion von Produktionssystemen und IoT-Geräten

Neben klassischen IT-Systemen werden vermehrt auch Geräte durch Schadprogramme angegriffen, die auf den ersten Blick nicht wie offensichtliche Ziele aussehen. Bei einem Angriff könnte beispielsweise eine über das Internet erreichbare Überwachungskamera infiziert werden, um in der Institution zu spionieren. Aber auch eine vernetzte Glühbirne oder eine Kaffeemaschine mit App-Steuerung kann als Eintrittspunkt in das Netz der Institution oder als Teil eines Botnetzes dienen, wenn diese Geräte nicht ausreichend vor Schadprogrammen geschützt werden. Vernetzte Produktionssysteme oder Industriesteuerungen können ebenfalls durch Schadprogramme manipuliert oder sogar zerstört werden, was Ausfälle und viele weitere Gefährdungen für die Institution und ihre Mitarbeitenden, z. B. durch Brände, nach sich ziehen kann.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins OPS.*1.1.4 Schutz vor Schadprogrammen* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeiten	Rollen
Grundsätzlich zuständig	IT-Betrieb
Weitere Zuständigkeiten	Benutzende

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

OPS.1.1.4.A1 Erstellung eines Konzepts für den Schutz vor Schadprogrammen (B)

Es MUSS ein Konzept erstellt werden, das beschreibt, welche IT-Systeme vor Schadprogrammen geschützt werden müssen. Hierbei MÜSSEN auch IoT-Geräte und Produktionssysteme berücksichtigt werden. Außerdem MUSS festgehalten werden, wie der Schutz zu erfolgen hat. Ist kein verlässlicher Schutz möglich, so SOLLTEN die identifizierten IT-Systeme NICHT betrieben werden. Das Konzept SOLLTE nachvollziehbar dokumentiert und aktuell gehalten werden.

OPS.1.1.4.A2 Nutzung systemspezifischer Schutzmechanismen (B)

Es MUSS geprüft werden, welche Schutzmechanismen die verwendeten IT-Systeme sowie die darauf genutzten Betriebssysteme und Anwendungen bieten. Diese Mechanismen MÜSSEN genutzt werden, sofern es keinen mindestens gleichwertigen Ersatz gibt oder gute Gründe dagegen sprechen. Werden sie nicht genutzt, MUSS dies begründet und dokumentiert werden.

OPS.1.1.4.A3 Auswahl eines Virenschutzprogrammes (B)

Abhängig vom verwendeten Betriebssystem, anderen vorhandenen Schutzmechanismen sowie der Verfügbarkeit geeigneter Virenschutzprogramme MUSS für den konkreten Einsatzzweck ein entsprechendes Schutzprogramm ausgewählt und installiert werden. Für Gateways und IT-Systeme, die dem Datenaustausch dienen, MUSS ein geeignetes Virenschutzprogramm ausgewählt und installiert werden.

Es DÜRFEN NUR Produkte für den Enterprise-Bereich mit auf die Institution zugeschnittenen Service- und Supportleistungen eingesetzt werden. Produkte für die reine Heimanwendung oder Produkte ohne Support DÜRFEN NICHT im professionellen Wirkbetrieb eingesetzt werden.

Cloud-Dienste zur Verbesserung der Detektionsleistung der Virenschutzprogramme SOLLTEN genutzt werden. Falls Cloud-Funktionen solcher Produkte verwendet werden, MUSS sichergestellt werden, dass dies nicht im Widerspruch zum Daten- oder Geheimschutz steht. Neben Echtzeit- und On-Demand-Scans MUSS eine eingesetzte Lösung die Möglichkeit bieten, auch komprimierte Daten nach Schadprogrammen zu durchsuchen.

OPS.1.1.4.A4 ENTFALLEN (B)

Diese Anforderung ist entfallen.

OPS.1.1.4.A5 Betrieb und Konfiguration von Virenschutzprogrammen (B)

Das Virenschutzprogramm MUSS für seine Einsatzumgebung geeignet konfiguriert werden. Die Erkennungsleistung SOLLTE dabei im Vordergrund stehen, sofern nicht Datenschutz- oder Leistungsgründe im jeweiligen Einzelfall dagegen sprechen. Wenn sicherheitsrelevante Funktionen des Virenschutzprogramms nicht genutzt werden, SOLLTE dies begründet und dokumentiert werden. Bei Schutzprogrammen, die speziell für die Desktop-Virtualisierung optimiert sind, SOLLTE nachvollziehbar dokumentiert sein, ob auf bestimmte Detektionsverfahren zugunsten der Leistung verzichtet wird. Es MUSS sichergestellt werden, dass die Benutzenden keine sicherheitsrelevanten Änderungen an den Einstellungen der Antivirenprogramme vornehmen können.

OPS.1.1.4.A6 Regelmäßige Aktualisierung der eingesetzten Virenschutzprogramme (B)

Auf den damit ausgestatteten IT-Systemen MÜSSEN die Virenschutzprogramme nach Empfehlung der herstellenden Institution regelmäßig und zeitnah aktualisiert werden.

OPS.1.1.4.A7 Sensibilisierung und Verpflichtung der Benutzenden (B) [Benutzende]

Benutzende MÜSSEN regelmäßig über die Bedrohung durch Schadprogramme aufgeklärt werden. Sie MÜSSEN die grundlegenden Verhaltensregeln einhalten, um die Gefahr eines Befalls durch Schadprogramme zu reduzieren. Dateien, E-Mails, Webseiten usw. aus nicht vertrauenswürdigen Quellen SOLLTEN NICHT geöffnet werden. Sie MÜSSEN entsprechenden Kontaktpersonen für den Fall eines Verdacht auf eine Infektion mit einem Schadprogramm bekannt sein. Sie MÜSSEN sich an die ihnen benannten Kontaktpersonen wenden, wenn der Verdacht auf eine Infektion mit einem Schadprogramm besteht.

3.2. Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für diesen Baustein. Sie SOLLTEN grundsätzlich erfüllt werden.

OPS.1.1.4.A8 ENTFALLEN (S)

Diese Anforderung ist entfallen.

OPS.1.1.4.A9 Meldung von Infektionen mit Schadprogrammen (S) [Benutzende]

Das eingesetzte Virenschutzprogramm SOLLTE eine Infektion mit einem Schadprogramm automatisch blockieren und melden. Die automatische Meldung SOLLTE an einer zentralen Stelle angenommen werden. Dabei SOLLTEN die zuständigen Mitarbeitenden je nach Sachlage über das weitere Vorgehen entscheiden. Das Vorgehen bei Meldungen und Alarmen der Virenschutzprogramme SOLLTE geplant, dokumentiert und getestet werden. Es SOLLTE insbesondere geregelt sein, was im Falle einer bestätigten Infektion geschehen soll.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

OPS.1.1.4.A10 Nutzung spezieller Analyseumgebungen (H)

Automatisierte Analysen in einer speziellen Testumgebung (basierend auf Sandboxen bzw. separaten virtuellen oder physischen Systemen) SOLLTEN für eine Bewertung von verdächtigen Dateien ergänzend herangezogen werden.

OPS.1.1.4.A11 Einsatz mehrerer Scan-Engines (H)

Zur Verbesserung der Erkennungsleistung SOLLTEN für besonders schutzwürdige IT-Systeme, wie Gateways und IT-Systeme zum Datenaustausch, Virenschutzprogramme mit mehreren alternativen Scan-Engines eingesetzt werden.

OPS.1.1.4.A12 Einsatz von Datenträgerschleusen (H)

Bevor insbesondere Datenträger von Dritten mit den IT-Systemen der Institution verbunden werden, SOLLTEN diese durch eine Datenträgerschleuse geprüft werden.

OPS.1.1.4.A13 Umgang mit nicht vertrauenswürdigen Dateien (H)

Ist es notwendig, nicht vertrauenswürdige Dateien zu öffnen, SOLLTE dies nur auf einem isolierten IT-System geschehen. Die betroffenen Dateien SOLLTEN dort z. B. in ein ungefährliches Format umgewandelt oder ausgedruckt werden, wenn sich hierdurch das Risiko einer Infektion durch Schadsoftware verringert.

OPS.1.1.4.A14 Auswahl und Einsatz von Cyber-Sicherheitsprodukten gegen gezielte Angriffe (H)

Der Einsatz sowie der Mehrwert von Produkten und Services, die im Vergleich zu herkömmlichen Virenschutzprogrammen einen erweiterten Schutzumfang bieten, SOLLTE geprüft werden. Solche Sicherheitsprodukte gegen gezielte Angriffe SOLLTEN z. B. bei der Ausführung von Dateien in speziellen Analyseumgebungen, bei der Härtung von Clients oder bei der Kapselung von Prozessen eingesetzt werden. Vor einer Kaufentscheidung für ein Sicherheitsprodukt SOLLTEN Schutzwirkung und Kompatibilität zur eigenen IT-Umgebung getestet werden.

OPS.1.1.4.A15 ENTFALLEN (H)

Diese Anforderung ist entfallen.

4. Weiterführende Informationen

4.1. Wissenswertes

Die International Organization for Standardization (ISO) gibt in der Norm ISO/IEC 27001:2013, insbesondere in Annex A, A.12.2 „protection from malware", Vorgaben für den Schutz vor Schadprogrammen.

Das Information Security Forum (ISF) macht in seinem Standard „The Standard of Good Practice for Information Security", insbesondere Area TS1 Security Solutions, Vorgaben für den Schutz vor Schadprogrammen.

Bundesamt
für Sicherheit in der
Informationstechnik

OPS.1.1.5 Protokollierung

1. Beschreibung

1.1. Einleitung

Damit ein verlässlicher IT-Betrieb gewährleistet ist, sollten IT-Systeme und Anwendungen entweder alle oder zumindest ausgewählte betriebs- und sicherheitsrelevante Ereignisse protokollieren, d. h. sie automatisch speichern und für die Auswertung bereitstellen. Eine Protokollierung wird in vielen Institutionen eingesetzt, um Hard- und Softwareprobleme sowie Ressourcenengpässe rechtzeitig entdecken zu können. Aber auch Sicherheitsprobleme und Angriffe auf die betriebenen Netzdienste können anhand von Protokollierungsdaten nachvollzogen werden. Ebenso können mit solchen Daten durch forensische Untersuchungen Beweise gesichert werden, nachdem ein Angriff auf IT-Systeme oder Anwendungen bekannt wurde.

In jedem Informationsverbund werden lokal Protokollierungsdaten von einer Vielzahl von IT-Systemen und Anwendungen generiert. Um jedoch einen Gesamtüberblick über einen Informationsverbund zu erhalten, können die von verschiedenen IT-Systemen und Anwendungen generierten Protokollierungsereignisse an eine dedizierte Protokollierungsinfrastruktur gesendet und dort zentral gespeichert werden. Nur so lassen sich die Protokollierungsdaten an einer zentralen Stelle auswählen, filtern und systematisch auswerten.

1.2. Zielsetzung

Ziel des Bausteins ist es, alle relevanten Daten sicher zu erheben, zu speichern und geeignet für die Auswertung bereitzustellen, damit möglichst alle sicherheitsrelevanten Ereignisse protokolliert werden können.

1.3. Abgrenzung und Modellierung

Der Baustein OPS.1.1.5 *Protokollierung* ist einmal auf den gesamten Informationsverbund anzuwenden.

Im vorliegenden Baustein werden ausschließlich übergreifende Aspekte betrachtet, die für eine angemessene Protokollierung erforderlich sind. Die Protokollierung spezifischer IT-Systeme oder Anwendungen wird hier nicht behandelt, sondern in den jeweiligen Bausteinen des IT-Grundschutz-Kompendiums beschrieben.

In vielen Betriebssystemen oder Anwendungen sind Protokollierungsfunktionen bereits vorhanden oder können dort mittels Zusatzprodukten integriert werden. Um diese Funktionen und die gespeicherten Protokollierungsdaten abzusichern, muss das zugrundeliegende Betriebssystem geschützt sein. Das ist jedoch nicht Bestandteil dieses Bausteins. Dafür sind die betriebssystemspezifischen Bausteine umzusetzen, z. B. SYS.1.2.3 *Windows Server*.

Im Vorfeld der Protokollierung von sicherheitsrelevanten Ereignissen ist es wichtig, dass Zuständigkeiten und Kompetenzen klar definiert und zugewiesen werden. Es sollte insbesondere auf den Grundsatz der Funktionstrennung geachtet werden. Dieses Thema ist nicht Bestandteil dieses Bausteins, sondern wird im Baustein ORP.1 *Organisation* behandelt.

Auch ist dieser Baustein abzugrenzen von der Detektion von sicherheitsrelevanten Ereignissen (siehe DER.1 *Detektion von sicherheitsrelevanten Ereignissen*) sowie der Reaktion auf Sicherheitsvorfälle (siehe DER.2.1 *Behandlung von Sicherheitsvorfällen*). Beide Aspekte werden im vorliegenden Baustein nicht oder nur am Rande behandelt.

Ebenfalls an anderer Stelle beschrieben werden die Auswertung von Protokollierungsdaten sowie deren langfristige, sichere, unveränderbare und reproduzierbare Speicherung (siehe DER.1 *Detektion von sicherheitsrelevanten Ereignissen* bzw. OPS.1.2.2 *Archivierung*).

Vorgaben, wie mit personenbezogenen Daten umzugehen ist, werden im Baustein CON.2 *Datenschutz* beschrieben.

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein OPS.1.1.5 *Protokollierung* von besonderer Bedeutung.

2.1. Fehlende oder unzureichende Protokollierung

In einem Informationsverbund gibt es häufig IT-Systeme oder Anwendungen, bei denen die Protokollierung in der Grundeinstellung nicht aktiviert wurde. Auch können einzelne IT-Systeme oder Anwendungen manchmal gar nicht protokollieren. In beiden Fällen können wichtige Informationen verloren gehen und Angriffe nicht rechtzeitig erkannt werden. Das ist auch dann möglich, wenn die Protokollierung bei einzelnen IT-Systemen oder Anwendungen zwar genutzt wird, aber die Protokollierungsdaten nicht an einer zentralen Stelle zusammengeführt werden. In Informationsverbünden ohne zentrale Protokollierung lässt sich schwer sicherstellen, dass die relevanten Protokollinformationen aller IT-Systeme und Anwendungen erhalten bleiben und ausgewertet werden.

Weiterhin müssen Protokollierungsdaten aussagekräftige Informationen enthalten. Welche Ereignisse protokolliert werden, hängt unter anderem auch vom Schutzbedarf der jeweiligen IT-Systeme oder Anwendungen ab. Wird dieser missachtet, indem beispielsweise bei der Protokollierung nur auf Standard-Einstellungen der IT-Systeme bzw. Anwendungen zurückgegriffen wird, kann dies dazu führen, dass besonders relevante Sicherheitsereignisse nicht protokolliert werden. Somit werden Angriffe eventuell nicht erkannt.

2.2. Fehlerhafte Auswahl von relevanten Protokollierungsdaten

Protokollierungsdaten liefern oft wichtige Informationen, die dabei helfen, Sicherheitsvorfälle zu erkennen. Eine besondere Herausforderung ist es, die relevanten Meldungen aus der großen Menge der verschiedenen Protokollierungsereignisse herauszufiltern. Denn viele Protokollierungsereignisse haben nur informativen Charakter und lenken von den wirklich wichtigen Meldungen ab. Werden zu viele Protokollierungsereignisse ausgewählt, lässt sich die Fülle an Informationen nur schwer und mit hohem Zeitaufwand auswerten.

Des Weiteren können Protokollierungsereignisse verworfen oder überschrieben werden, wenn der Arbeitsspeicher oder die Festplattenkapazität des IT-Systems bzw. der Protokollierungsinfrastruktur nicht ausreichen. Werden dadurch zu wenige oder nicht ausreichend relevante Protokollierungsereignisse aufgezeichnet, dann könnten sicherheitskritische Vorfälle unerkannt bleiben.

2.3. Fehlende oder fehlerhafte Zeitsynchronisation bei der Protokollierung

Wenn in einem Informationsverbund die Zeit nicht auf allen IT-Systemen synchronisiert wird, können die Protokollierungsdaten eventuell nicht miteinander korreliert werden bzw. kann die Korrelation eventuell zu fehlerhaften Aussagen führen. Grund dafür ist, dass die unterschiedlichen Zeitstempel von Ereignissen keine gemeinsame Basis aufweisen. Eine fehlende Zeitsynchronisation erschwert es somit, erhobene Protokollierungsdaten auszuwerten, insbesondere, wenn diese auf einem zentralen Logserver gespeichert werden. Weiterhin kann eine fehlerhafte oder fehlende Zeitsynchronisation dazu führen, dass die Protokollierung nicht zur Beweissicherung herangezogen werden kann.

2.4. Fehlplanung bei der Protokollierung

Wird die Protokollierung nicht ausreichend geplant, dann kann dies dazu führen, dass IT-Systeme oder Anwendungen nicht überwacht und sicherheitsrelevante Ereignisse somit nicht erkannt und angemessen behandelt werden. Datenschutzverstöße könnten ebenfalls nicht nachvollzogen werden.

2.5. Vertraulichkeits- und Integritätsverlust von Protokollierungsdaten

Einige IT-Systeme in einem Informationsverbund generieren Protokollierungsdaten wie Anmeldenamen, IP-Adressen, E-Mail-Adressen und Rechnernamen, die konkreten Personen zugeordnet werden können. Solche Informationen lassen sich kopieren, abhören und manipulieren, wenn sie nicht verschlüsselt übertragen und gesichert gespeichert werden. Dies kann dazu führen, dass Angreifende auf vertrauliche Informationen zugreifen oder dass, durch manipulierte Protokollierungsdaten, Sicherheitsvorfälle bewusst verschleiert werden. Ebenso können Angreifende, wenn sie an eine größere Menge von Protokollierungsdaten gelangen, diese Informationen nutzen, um die interne Struktur des Informationsverbunds aufzudecken und dadurch ihre Angriffe gezielter ausrichten.

2.6. Falsch konfigurierte Protokollierung

Wenn die Protokollierung in IT-Systemen falsch konfiguriert ist, werden wichtige Informationen entweder fehlerhaft oder gar nicht aufgezeichnet. Auch kann es sein, dass zu viele oder falsche Informationen protokolliert werden. So können z. B. personenbezogene Daten unberechtigt protokolliert und gespeichert werden. Die Institution könnte dadurch gegen gesetzliche Anforderungen verstoßen.

Durch eine falsch konfigurierte Protokollierung ist es ebenso möglich, dass die Protokollierungsdaten in inkonsistenten oder proprietären Formaten vorliegen. Dadurch lassen sich die Protokolle eventuell nur schwer auswerten und Sicherheitsvorfälle bleiben unentdeckt.

2.7. Ausfall von Datenquellen für Protokollierungsdaten

Liefern IT-Systeme in einem Informationsverbund nicht mehr die notwendigen Protokollierungsdaten, lassen sich Sicherheitsvorfälle nicht mehr angemessen detektieren. Ursache für solche Ausfälle von Datenquellen können Fehler in der Hard- und Software oder auch fehlerhaft administrierte IT-Systeme sein. Besonders, wenn nicht bemerkt wird, dass Datenquellen ausgefallen sind, kann dies zu einem falschen Bild der Sicherheitslage in der Institution führen. Dadurch können Angreifende z. B. sehr lange unbemerkt bleiben und institutionskritische Informationen abgreifen oder Produktionssysteme manipulieren.

2.8. Ungenügend dimensionierte Protokollierungsinfrastruktur

Aufgrund der komplexen Informationsverbünde und der vielfältigen Angriffsszenarien steigen die Anforderungen an die Protokollierung, da sehr viele Protokollierungsdaten gespeichert und verarbeitet werden müssen. Weiterhin ist es bei Sicherheitsvorfällen üblich, die Intensität der Protokollierung zu erhöhen. Ist die Protokollierungsinfrastruktur dafür jedoch nicht ausgelegt, kann es passieren, dass Protokollierungsdaten unvollständig gespeichert werden. Somit lassen sich sicherheitsrelevante Ereignisse nicht mehr oder nur unzureichend auswerten und Sicherheitsvorfälle bleiben unentdeckt.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins OPS.1.1.5 *Protokollierung* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeiten	Rollen
Grundsätzlich zuständig	IT-Betrieb
Weitere Zuständigkeiten	Fachverantwortliche

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

OPS.1.1.5.A1 Erstellung einer Sicherheitsrichtlinie für die Protokollierung (B) [Fachverantwortliche]

Ausgehend von der allgemeinen Sicherheitsrichtlinie der Institution MUSS eine spezifische Sicherheitsrichtlinie für die Protokollierung erstellt werden. In dieser Sicherheitsrichtlinie MÜSSEN nachvollziehbar Anforderungen und Vorgaben beschrieben sein, wie die Protokollierung zu planen, aufzubauen und sicher zu betreiben ist. In der spezifischen Sicherheitsrichtlinie MUSS geregelt werden, wie, wo und was zu protokollieren ist. Dabei SOLLTEN sich Art und Umfang der Protokollierung am Schutzbedarf der Informationen orientieren.

Die spezifische Sicherheitsrichtlinie MUSS von dem oder der ISB gemeinsam mit den Fachverantwortlichen erstellt werden. Sie MUSS allen für die Protokollierung zuständigen Mitarbeitenden bekannt und grundlegend für ihre Arbeit sein. Wird die spezifische Sicherheitsrichtlinie verändert oder wird von den Anforderungen abgewichen, MUSS dies mit dem oder der ISB abgestimmt und dokumentiert werden. Es MUSS regelmäßig überprüft werden, ob die spezifische Sicherheitsrichtlinie noch korrekt umgesetzt ist. Die Ergebnisse der Überprüfung MÜSSEN dokumentiert werden.

OPS.1.1.5.A2 ENTFALLEN (B)

Diese Anforderung ist entfallen.

OPS.1.1.5.A3 Konfiguration der Protokollierung auf System- und Netzebene (B)

Alle sicherheitsrelevanten Ereignisse von IT-Systemen und Anwendungen MÜSSEN protokolliert werden. Sofern die in der Protokollierungsrichtlinie als relevant definierten IT-Systeme und Anwendungen über eine Protokollierungsfunktion verfügen, MUSS diese benutzt werden. Wenn die Protokollierung eingerichtet wird, MÜSSEN dabei die Vorgaben des herstellenden Unternehmens für die jeweiligen IT-Systeme oder Anwendungen beachtet werden.

In angemessenen Intervallen MUSS stichpunktartig überprüft werden, ob die Protokollierung noch korrekt funktioniert. Die Prüfintervalle MÜSSEN in der Protokollierungsrichtlinie definiert werden.

Falls betriebs- und sicherheitsrelevante Ereignisse nicht auf einem IT-System protokolliert werden können, MÜSSEN zusätzliche IT-Systeme zur Protokollierung (z. B. von Ereignissen auf Netzebene) integriert werden.

OPS.1.1.5.A4 Zeitsynchronisation der IT-Systeme (B)

Die Systemzeit aller protokollierenden IT-Systeme und Anwendungen MUSS immer synchron sein. Es MUSS sichergestellt sein, dass das Datums- und Zeitformat der Protokolldateien einheitlich ist.

OPS.1.1.5.A5 Einhaltung rechtlicher Rahmenbedingungen (B)

Bei der Protokollierung MÜSSEN die Bestimmungen aus den aktuellen Gesetzen zum Bundes- sowie Landesdatenschutz eingehalten werden (siehe CON.2 *Datenschutz*).

Darüber hinaus MÜSSEN eventuelle Persönlichkeitsrechte bzw. Mitbestimmungsrechte der Mitarbeitendenvertretungen gewahrt werden.

Ebenso MUSS sichergestellt sein, dass alle weiteren relevanten gesetzlichen Bestimmungen beachtet werden.

Protokollierungsdaten MÜSSEN nach einem festgelegten Prozess gelöscht werden. Es MUSS technisch unterbunden werden, dass Protokollierungsdaten unkontrolliert gelöscht oder verändert werden.

3.2. Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für diesen Baustein. Sie SOLLTEN grundsätzlich erfüllt werden.

OPS.1.1.5.A6 Aufbau einer zentralen Protokollierungsinfrastruktur (S)

Alle gesammelten sicherheitsrelevanten Protokollierungsdaten SOLLTEN an einer zentralen Stelle gespeichert werden. Dafür SOLLTE eine zentrale Protokollierungsinfrastruktur im Sinne eines Logserver-Verbunds aufgebaut und in einem hierfür eingerichteten Netzsegment platziert werden (siehe NET.1.1 *Netzarchitektur und -design*).

Zusätzlich zu sicherheitsrelevanten Ereignissen (siehe OPS.1.1.5.A3 *Konfiguration der Protokollierung auf System- und Netzebene*) SOLLTE eine zentrale Protokollierungsinfrastruktur auch allgemeine Betriebsereignisse protokollieren, die auf einen Fehler hindeuten.

Die Protokollierungsinfrastruktur SOLLTE ausreichend dimensioniert sein. Die Möglichkeit einer Skalierung im Sinne einer erweiterten Protokollierung SOLLTE berücksichtigt werden. Dafür SOLLTEN genügend technische, finanzielle und personelle Ressourcen verfügbar sein.

OPS.1.1.5.A7 ENTFALLEN (S)

Diese Anforderung ist entfallen.

OPS.1.1.5.A8 Archivierung von Protokollierungsdaten (S)

Protokollierungsdaten SOLLTEN archiviert werden. Dabei SOLLTEN die gesetzlich vorgeschriebenen Regelungen berücksichtigt werden.

OPS.1.1.5.A9 Bereitstellung von Protokollierungsdaten für die Auswertung (S)

Die gesammelten Protokollierungsdaten SOLLTEN gefiltert, normalisiert, aggregiert und korreliert werden. Die so bearbeiteten Protokollierungsdaten SOLLTEN geeignet verfügbar gemacht werden, damit sie ausgewertet werden können.

Damit sich die Daten automatisiert auswerten lassen, SOLLTEN die Protokollanwendungen über entsprechende Schnittstellen für die Auswertungsprogramme verfügen.

Es SOLLTE sichergestellt sein, dass bei der Auswertung von Protokollierungsdaten die Sicherheitsanforderungen eingehalten werden, die in der Protokollierungsrichtlinie definiert sind. Auch wenn die Daten bereitgestellt werden, SOLLTEN betriebliche und interne Vereinbarungen berücksichtigt werden.

Die Protokollierungsdaten SOLLTEN zusätzlich in unveränderter Originalform aufbewahrt werden.

OPS.1.1.5.A10 Zugriffsschutz für Protokollierungsdaten (S)

Es SOLLTE sichergestellt sein, dass die ausführenden Administrierenden selbst keine Berechtigung haben, die aufgezeichneten Protokollierungsdaten zu verändern oder zu löschen.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

OPS.1.1.5.A11 Steigerung des Protokollierungsumfangs (H)

Bei erhöhtem Schutzbedarf von Anwendungen oder IT-Systemen SOLLTEN grundsätzlich mehr Ereignisse protokolliert werden, sodass sicherheitsrelevante Vorfälle möglichst lückenlos nachvollziehbar sind.

Um die Protokollierungsdaten in Echtzeit auswerten zu können, SOLLTEN sie in verkürzten Zeitabständen von den protokollierenden IT-Systemen und Anwendungen zentral gespeichert werden. Die Protokollierung SOLLTE eine Auswertung über den gesamten Informationsverbund ermöglichen. Anwendungen und IT-Systeme, mit denen eine zentrale Protokollierung nicht möglich ist, SOLLTEN bei einem erhöhten Schutzbedarf NICHT eingesetzt werden.

OPS.1.1.5.A12 Verschlüsselung der Protokollierungsdaten (H)

Um Protokollierungsdaten sicher übertragen zu können, SOLLTEN sie verschlüsselt werden. Alle gespeicherten Protokolle SOLLTEN digital signiert werden. Auch archivierte und außerhalb der Protokollierungsinfrastruktur gespeicherte Protokollierungsdaten SOLLTEN immer verschlüsselt gespeichert werden.

OPS.1.1.5.A13 Hochverfügbare Protokollierungsinfrastruktur (H)

Eine hochverfügbare Protokollierungsinfrastruktur SOLLTE aufgebaut werden.

4. Weiterführende Informationen

4.1. Wissenswertes

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) regelt in seinem Mindeststandard „Mindeststandard des BSI zur Protokollierung und Detektion von Cyber-Angriffen“ die Protokollierung und Detektion von sicherheitsrelevanten Ereignissen (SRE). Die Mindeststandards sind von den in § 8 Abs. 1 Satz 1 BSIG genannten Stellen der Bundesverwaltung umzusetzen.

Die International Organization for Standardization (ISO) macht in der Norm ISO/IEC 27001:2013 im Kapitel A.12.4 „Protokollierung und Überwachung“ Vorgaben zur Protokollierung.

Das Information Security Forum (ISF) macht in seinem Standard „The Standard of Good Practice for Information Security“ in Kapitel TM1.2 – Security Event Logging – Vorgaben zur Protokollierung.

Das National Institute of Standards and Technology (NIST) beschreibt in seiner Special Publication 800-92 „Guide to Computer Security Log Management“, wie Protokollierung sicher eingesetzt werden kann.

Bundesamt
für Sicherheit in der
Informationstechnik

OPS.1.1.6 Software-Tests und -Freigaben

1. Beschreibung

1.1. Einleitung

Der Einsatz von IT in Institutionen setzt voraus, dass die maschinelle Datenverarbeitung soweit wie möglich fehlerfrei funktioniert, da die Einzelergebnisse in den meisten Fällen nicht mehr kontrolliert werden können. Deswegen muss Software jeglicher Art schon vor Inbetriebnahme im Rahmen von Software-Tests überprüft werden. In diesen Tests muss nachgewiesen werden, dass die Software die erforderlichen Funktionen zuverlässig bereitstellt und darüber hinaus keine unerwünschten Nebeneffekte aufweist. Mit der anschließenden Freigabe der Software durch die fachlich zuständige Organisationseinheit wird die grundsätzliche Erlaubnis erteilt, die Software produktiv in der Institution zu nutzen. Gleichzeitig übernimmt diese Organisationseinheit damit auch die Verantwortung für das IT-Verfahren, das durch die Software unterstützt wird.

Software kann an unterschiedlichen Stellen ihres Lebenszyklus getestet werden. So können Software-Tests bereits bei der Entwicklung, vor der Freigabe für den Produktivbetrieb oder im Zuge des Patch- und Änderungsmanagements notwendig werden. Dies betrifft sowohl Individualsoftware als auch standardisierte Software. Eine besondere Rolle nehmen hierbei Regressionstests ein, denn selbst wenn nur kleinere Aspekte der Software geändert werden, besteht die Möglichkeit, dass sich dies auf ganz andere Aspekte und Funktionen der Software auswirkt. Regressionstests überprüfen Software genau auf diese Auswirkungen hin.

Dieser Baustein beschreibt den Test- und Freigabeprozess für jegliche Art von Software. Der Test- und Freigabeprozess zeichnet sich dadurch aus, dass dieser je nach Ergebnis mehrmals durchlaufen werden kann.

1.2. Zielsetzung

Mit der Umsetzung dieses Bausteins sorgt die Institution dafür, dass die eingesetzte Software den technischen und organisatorischen Anforderungen sowie dem vorliegenden Schutzbedarf der gesamten Institution oder einzelner Organisationseinheiten entspricht. Ein wesentlicher Teilaspekt ist dabei, dass sicherheitskritische Software auf bestehende Schwachstellen systematisch und methodisch überprüft wird.

1.3. Abgrenzung und Modellierung

Der Baustein OPS.1.1.6 *Software-Tests und Freigaben* ist auf den Informationsverbund einmal anzuwenden.

Während der Baustein CON.8 *Software-Entwicklung* auf den Softwareentwicklungsprozess und die darin enthaltenen Software-Tests, die während des Entwicklungsprozesses notwendig sind, eingeht, beschreibt dieser Baustein die speziellen Anforderungen, die an ein Test- und Freigabemanagement gestellt werden. Dabei bezieht sich dieses Test- und Freigabemanagement nicht ausschließlich auf selbst oder im Auftrag der Kundschaft entwickelte Software, sondern auch auf das Testen und die Freigabe von jeglicher Software, wie sie in APP.6 *Allgemeine Software* beschrieben wird, sowie alle weiteren Softwareprodukten der Schicht APP *Anwendungen*.

Software-Tests können auch Bestandteil des Patch- oder Änderungsmanagements oder der Software-Entwicklung werden. Entsprechende Anforderungen sind im Baustein OPS.1.1.3 *Patch- und Änderungsmanagement* sowie CON.8 *Software-Entwicklung* näher spezifiziert.

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein OPS.*1.1.6 Software-Tests und -Freigaben* von besonderer Bedeutung.

2.1. Software-Tests mit Produktivdaten

Werden Software-Tests mit Produktivdaten durchgeführt, können hierdurch Sicherheitsprobleme entstehen. Insbesondere vertrauliche Produktivdaten könnten dabei von unbefugten Mitarbeitenden oder Dritten eingesehen werden, die mit dem jeweiligen Software-Test beauftragt wurden. Wird mit den „originalen" Produktivdaten getestet und nicht mit Kopien der Daten, könnten diese ungewollt geändert oder gelöscht werden.

Durch Software-Tests im Produktivbetrieb könnte der gesamte Betrieb massiv gestört werden. Denn Fehlfunktionen der zu testenden Software können sich auch auf andere Anwendungen und IT-Systeme auswirken, die dadurch ebenfalls gestört werden. Hinzu kommt, dass Software-Testende bewusst die Software im Grenzbereich testen und damit beabsichtigen, mögliche Fehler aufzudecken. Dies erhöht wiederum die Gefahr, dass der gesamte Betrieb gestört wird.

2.2. Fehlendes oder unzureichendes Testverfahren

Wird neue Software nicht oder nur unzureichend getestet und ohne Installationsvorschriften freigegeben, können Fehler in der Software unerkannt bleiben. Ebenso ist es möglich, dass dadurch erforderliche und einzuhaltende Installationsparameter nicht erkannt oder nicht beachtet werden.

Diese Software- oder Installationsfehler, die aus einem fehlenden oder unzureichenden Software-Testverfahren resultieren, können den IT-Betrieb der Institution erheblich gefährden. So können beispielsweise wichtige Daten verloren gehen, wenn ein Software-Update eingespielt wird.

2.3. Fehlendes oder unzureichendes Freigabeverfahren

Ein fehlendes oder unzureichendes Freigabeverfahren kann dazu führen, dass Software eingesetzt wird, die von der Fachseite nicht abgenommen wurde. Auf diese Weise kann die Software Funktionen umfassen, die sie nicht enthalten sollte, die nicht wie gewünscht funktionieren oder benötigte Funktionen können fehlen. Außerdem kann die Software zu anderen Anwendungen inkompatibel sein.

2.4. Fehlende oder unzureichende Dokumentation der Tests und Testergebnisse

Software kann in der Regel freigegeben werden, sobald alle Tests durchgeführt wurden und keine Abweichungen gefunden wurden. Sollte die Dokumentation der Software-Tests jedoch unvollständig sein, ist nachträglich nicht erkennbar, was getestet wurde. Wurden erkannte Softwarefehler oder fehlende Funktionen ungenügend dokumentiert und damit bei der Freigabe nicht berücksichtigt, können durch diese Abweichungen die zu verarbeitenden Produktivdaten ungewollt gelöscht oder verändert werden. Außerdem können andere IT-Systeme und Anwendungen gestört werden.

2.5. Fehlende oder unzureichende Dokumentation der Freigabekriterien

Wenn Freigabekriterien nicht klar kommuniziert werden, kann dies dazu führen, dass Software voreilig freigegeben wird oder keine Freigabe erfolgt, obwohl diese erteilt werden könnte. Dadurch könnten zum einen Versionen mit unerkannten Softwarefehlern freigegeben werden, die den Produktivbetrieb stören können. Zum anderen kann eine fehlende oder unzureichende Dokumentation der Freigabekriterien dazu führen, dass sich Projekte verzögern und dadurch finanzielle Schäden entstehen.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins OPS.1.1.6 *Software-Tests und -Freigaben* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.